

Modified planar functions and their components

Nurdagül Anbar¹, Wilfried Meidl²,

¹Technical University of Denmark,
Matematiktorvet, Building 303B, DK-2800, Lyngby, Denmark
Email: nurdagulanbar2@gmail.com

²Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences, Altenbergerstrasse 69, 4040-Linz, Austria
Email: meidlwilfried@gmail.com

Abstract

Zhou 2013 introduced modified planar functions to describe $(2^n, 2^n, 2^n, 1)$ relative difference sets R as a graph of a function on the finite field \mathbb{F}_{2^n} , and pointed out that projections of R are difference sets that can be described by negabent or bent₄ functions, which are Boolean functions given in multivariate form. Objective of this paper is to contribute to the understanding of these component functions of modified planar functions. We first completely describe a multivariate version of modified planar functions in terms of their bent₄ components. In the second part we characterize the component functions of (univariate) modified planar functions in terms of appropriate generalizations of the Walsh-Hadamard transform, with respect to which they have a flat spectrum. We hereby obtain a description of modified planar functions by their components which is similar to that of the classical planar functions in odd characteristic as a vectorial bent function.

1 Introduction

Let G be a group of order $\mu\nu$ and let N be a subgroup of G of order ν . A subset R of G of cardinality k is called a (μ, ν, k, λ) -relative difference set (RDS) of G relative to N , if every element of $G \setminus N$ can be written as a difference of two elements of R in exactly λ ways, and there is no such representation for any nonzero element in N . The subgroup N is hence

also called the forbidden subgroup. A powerful description of RDSs is their description via characters (see for instance Section 2.4. in [18]): A subset R of cardinality k of a group G of order $\mu\nu$ with a subgroup N of order ν is a (μ, ν, k, λ) -RDS of G relative to N if and only if for every character χ of G

$$|\chi(R)|^2 = \begin{cases} k^2 & \text{if } \chi = \chi_0, \\ k - \lambda\nu & \text{if } \chi \neq \chi_0, \text{ and } \chi(g) = 1 \text{ for all } g \in N, \\ k & \text{otherwise.} \end{cases} \quad (1)$$

As shown in [5, Theorem 3.1], an RDS relative to a normal subgroup N of G with parameters $(\mu, \nu, k, \lambda) = (q, q, q, 1)$ uniquely describes a projective plane, hence is of particular interest. For abelian groups G we have the following fundamental results on the existence of $(q, q, q, 1)$ -RDSs:

I : [1] If an abelian group G of odd order contains a $(q, q, q, 1)$ -RDS, then $q = p^n$ for some prime p and G contains an elementary abelian subgroup of order p^{n+1} .

II : [6] If an abelian group G of even order contains a $(q, q, q, 1)$ -RDS, then $q = 2^n$, $G \cong \mathbb{Z}_4^n$, and the forbidden subgroup is $2\mathbb{Z}_4^n$.

I: $|G| = q^2$ and q is odd.

All known $(q, q, q, 1)$ -RDSs are subsets of the $2n$ -dimensional vector space G over the finite field \mathbb{F}_p . As a result we can represent the group G as $G = (\mathbb{F}_p^n \times \mathbb{F}_p^n, +)$. In this case, $(q, q, q, 1)$ -RDSs can be expressed as the graph of a so-called *planar function* $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$,

$$R = \{(\mathbf{x}, f(\mathbf{x})) : \mathbf{x} \in \mathbb{F}_p^n\}.$$

Planar functions f are commonly defined by the property that the derivative in direction \mathbf{a}

$$D_{\mathbf{a}}f(\mathbf{x}) = f(\mathbf{x} + \mathbf{a}) - f(\mathbf{x})$$

is a permutation for all $\mathbf{a} \neq \mathbf{0}$. Planar functions have been widely studied since their introduction in [2].

Observe that the group of characters of $(\mathbb{F}_p^n \times \mathbb{F}_p^n, +)$ is

$$\{\chi_{\mathbf{u}, \mathbf{c}} : \mathbf{c}, \mathbf{u} \in \mathbb{F}_p^n\} \quad \text{with} \quad \chi_{\mathbf{u}, \mathbf{c}}(\mathbf{x}, \mathbf{y}) := \epsilon_p^{\mathbf{c} \cdot \mathbf{y} - \mathbf{u} \cdot \mathbf{x}},$$

where $\epsilon_p = e^{\frac{2\pi i}{p}}$ and $\mathbf{x} \cdot \mathbf{y}$ is the standard dot product of \mathbf{x} and \mathbf{y} . By the characterization of RDSs via characters, the set $R = \{(\mathbf{x}, f(\mathbf{x})) : \mathbf{x} \in \mathbb{F}_p^n\}$

for $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ is an RDS of $(\mathbb{F}_p^n \times \mathbb{F}_p^n, +)$ (relative to the subgroup $\{\mathbf{0}\} \times \mathbb{F}_p^n$) if and only if

$$|\chi_{\mathbf{u}, \mathbf{c}}(R)|^2 = \left| \sum_{\mathbf{x} \in \mathbb{F}_p^n} \epsilon_p^{\mathbf{c} \cdot f(\mathbf{x}) - \mathbf{u} \cdot \mathbf{x}} \right|^2 =: |\mathcal{W}_{\mathbf{c}, f}(\mathbf{u})|^2 = p^n \quad (2)$$

for all $\mathbf{u} \in \mathbb{F}_p^n$ and nonzero $\mathbf{c} \in \mathbb{F}_p^n$. As is well known, the character sum in Equation (2) is called the *Walsh-Hadamard transform* of the function $\mathbf{c} \cdot f(\mathbf{x}) =: f_{\mathbf{c}}(\mathbf{x})$ from \mathbb{F}_p^n to \mathbb{F}_p , which (for nonzero \mathbf{c}) is called a *component function* of f . Moreover $g : \mathbb{F}_p^n \rightarrow \mathbb{F}_p$ is called a *(p-ary) bent function* if $|\mathcal{W}_g(\mathbf{u})|^2 = p^n$ for every $\mathbf{u} \in \mathbb{F}_p^n$, see [7]. We see that for all nonzero \mathbf{c} , the component function $f_{\mathbf{c}}$ of a planar function f is bent. In fact we have the following theorem, see e.g. [11, Theorem 3.19].

Theorem 1. *The function $f : \mathbb{F}_p^n \rightarrow \mathbb{F}_p^n$ is planar if and only if all its component functions $f_{\mathbf{c}}$ are bent.*

For the equivalent representation of G as $G = (\mathbb{F}_{p^n} \times \mathbb{F}_{p^n}, +)$, the RDS can be represented as a graph of a univariate function $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$. The Walsh transform of the component function $f_c(x) = \text{Tr}_n(cf(x))$ is then given by

$$\mathcal{W}_{f_c}(u) = \sum_{x \in \mathbb{F}_{p^n}} \epsilon_p^{\text{Tr}_n(cf(x)) - \text{Tr}_n(ux)},$$

where $\text{Tr}_n(z)$ denotes the absolute trace of $z \in \mathbb{F}_{p^n}$. All known planar functions are represented in univariate form and except from one example, they are all quadratic functions (Dembowski-Ostrom polynomials), see [11, Section 8].

II: $|G| = q^2$ and q is even.

Recently, in the significant contribution [20], Zhou presented a solution how to describe a $(2^n, 2^n, 2^n, 1)$ -RDS in \mathbb{Z}_4^n as a graph of a multivariate function f from \mathbb{F}_2^n to \mathbb{F}_2^n , respectively of a univariate function f on \mathbb{F}_{2^n} .

In the multivariate case, the group $G \cong \mathbb{Z}_4^n$ is represented as $G = (\mathbb{F}_2^n \times \mathbb{F}_2^n, *)$ where $(\mathbf{x}_1, \mathbf{y}_1) * (\mathbf{x}_2, \mathbf{y}_2) = (\mathbf{x}_1 + \mathbf{x}_2, \mathbf{y}_1 + \mathbf{y}_2 + \mathbf{x}_1 \odot \mathbf{x}_2)$ with $(x_1, x_2, \dots, x_n) \odot (y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n)$. The graph of a function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is then an RDS in G relative to $\{\mathbf{0}\} \times \mathbb{F}_2^n \cong 2\mathbb{Z}_4^n$ if and only if

$$f(\mathbf{x} + \mathbf{a}) + f(\mathbf{x}) + \mathbf{a} \odot \mathbf{x} \quad (3)$$

is a permutation for every nonzero $\mathbf{a} \in \mathbb{F}_2^n$.

Alternatively we can represent \mathbb{Z}_4^n as $G = (\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \star)$ where the group operation is given by $(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + x_1 x_2)$. In this case the graph of the univariate function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is an RDS in G (relative to $\{0\} \times \mathbb{F}_{2^n}$) if and only if

$$f(x + a) + f(x) + ax \quad (4)$$

is a permutation for every nonzero $a \in \mathbb{F}_{2^n}$.

In accordance with [11], we call multivariate functions on \mathbb{F}_2^n for which (3) is always a permutation, respectively univariate functions on \mathbb{F}_{2^n} for which (4) is always a permutation, *modified planar functions*.

We emphasize that the multivariate modified planar functions for the group $(\mathbb{F}_2^n \times \mathbb{F}_2^n, *)$ are not the one-to-one translation of the univariate modified planar functions for the group $(\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \star)$ by choosing an appropriate basis for \mathbb{F}_{2^n} . For details we refer to [20], where both versions were introduced. One can see that in detail they can behave quite differently, observing that every affine function from \mathbb{F}_{2^n} to \mathbb{F}_{2^n} is a trivial example of a univariate modified planar function. In particular, the zero-function on \mathbb{F}_{2^n} is modified planar. This obviously is not the case for the zero function on \mathbb{F}_2^n .

The component functions of modified planar functions correspond to $(2^n, 2, 2^n, 2^{n-1})$ -RDSs in $\mathbb{Z}_4 \times \mathbb{Z}_2^{n-1}$, which essentially can be represented by the graph of a *negabent function* (or more general a *bent₄* function, which is also called a *shifted bent* function), see the discussions in [20, Section 5] and [10, Section 7]. One of the objectives of this paper is to contribute to the understanding of the component functions of modified planar functions.

Many interesting results on modified planar functions such as relations to semifields, which are analogues of the results on planar functions in odd characteristic, have been discovered. For more detailed information we refer to [10, 15, 20], and the excellent recent overview paper [11].

Objective of this paper is to contribute to the understanding of the component functions of modified planar functions. In Section 2, we first recall *bent₄* functions, which have been defined and analysed as multivariate Boolean functions with a flat spectrum with respect to certain unitary transforms. Then we elaborate connections between (multivariate) modified planar functions and *bent₄* functions, which were already pointed at in [20], in more detail. In Section 3 we characterize the component functions of univariate modified planar functions in terms of character sums, again unitary transforms, with respect to which they have a flat spectrum. Though they behave somewhat different than the multivariate *bent₄* functions, we suggest to call them (univariate) *bent₄* functions as well.

2 Components of multivariate modified planar functions

For the convenience of the reader we first set up some notation. We denote by \mathbb{C} the set of complex numbers, by \mathbb{F}_{2^n} the finite field of order 2^n and by \mathbb{F}_2^n the space of all n -tuples (x_1, \dots, x_n) of elements from \mathbb{F}_2 . In particular, we denote by $\mathbf{0}$ and $\mathbf{1}$ the n -tuples in \mathbb{F}_2^n whose entries are all 0 and 1, respectively.

For $\mathbf{c} = (c_1, \dots, c_n)$, $\mathbf{x} = (x_1, \dots, x_n)$ in \mathbb{F}_2^n , in accordance with the notation in [4] we set

$$s_2^{\mathbf{c}}(\mathbf{x}) := \bigoplus_{1 \leq i < j \leq n} (c_i x_i)(c_j x_j) .$$

Note that $s_2^{\mathbf{c}}(\mathbf{x}) = s_2(\mathbf{c} \odot \mathbf{x})$, where $s_2(x)$ is the homogeneous symmetric Boolean function with algebraic degree 2. For an element $\mathbf{c} \in \mathbb{F}_2^n$ and a Boolean function $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$, a unitary transform $\mathcal{U}_g^{\mathbf{c}} : \mathbb{F}_2^n \rightarrow \mathbb{C}$ is defined by (cf.[4])

$$\mathcal{U}_g^{\mathbf{c}}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) + s_2^{\mathbf{c}}(\mathbf{x})} i^{\mathbf{c} \cdot \mathbf{x}} (-1)^{\mathbf{u} \cdot \mathbf{x}} . \quad (5)$$

By [4, Proposition 3], for $\mathbf{c}, \mathbf{x} \in \mathbb{F}_2^n$ we have

$$\mathbf{c} \cdot \mathbf{x} + 2s_2^{\mathbf{c}}(\mathbf{x}) \equiv wt(\mathbf{c} \odot \mathbf{x}) \pmod{4}$$

where $wt(\mathbf{z})$ denotes the Hamming weight of $\mathbf{z} \in \mathbb{F}_2^n$. As a result we can write Equation (5) also as

$$\mathcal{U}_g^{\mathbf{c}}(\mathbf{u}) = \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{g(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}} i^{wt(\mathbf{c} \odot \mathbf{x})} . \quad (6)$$

Obviously, for $\mathbf{c} = \mathbf{0}$ the transform $\mathcal{U}_g^{\mathbf{0}}$ in Equation (6) is the conventional Walsh-Hadamard transform of g , and for $\mathbf{c} = \mathbf{1}$ it is known as the *negahadamard transform* of g , see [9].

Definition 2. A Boolean function $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is called *bent₄* if it has a flat spectrum with respect to at least one of the transforms $\mathcal{U}_g^{\mathbf{c}}$. In other words, g is *bent₄* if there exists an element $\mathbf{c} \in \mathbb{F}_2^n$ such that $|\mathcal{U}_g^{\mathbf{c}}(\mathbf{u})| = 2^{n/2}$ for all $\mathbf{u} \in \mathbb{F}_2^n$.

The Boolean functions with flat spectrum with respect to $\mathcal{U}_g^{\mathbf{0}}$ are the celebrated bent functions. If g is flat with respect to $\mathcal{U}_g^{\mathbf{1}}$, then g is called

negabent. We will call g a \mathbf{c} -bent₄ function if g has a flat spectrum with respect to $\mathcal{U}_g^{\mathbf{c}}$. Negabent functions have been investigated in [9, 14, 16, 17, 19], for more background on bent₄ functions we refer to [12], where they have been introduced, and to [4].

In this section we look at the relation between modified planar functions in multivariate form defined as in (3) and bent₄ functions in more detail.

Proposition 3. *Let $G = (\mathbb{F}_2^n \times \mathbb{F}_2^n, *)$ with*

$$(\mathbf{x}_1, \mathbf{y}_1) * (\mathbf{x}_2, \mathbf{y}_2) = (\mathbf{x}_1 + \mathbf{x}_2, \mathbf{y}_1 + \mathbf{y}_2 + \mathbf{x}_1 \odot \mathbf{x}_2) .$$

The group of characters of G is then $\chi_G = \{\chi_{\mathbf{u}, \mathbf{c}} : \mathbf{u}, \mathbf{c} \in \mathbb{F}_2^n\}$ where

$$\chi_{\mathbf{u}, \mathbf{c}}(\mathbf{x}, \mathbf{y}) = (-1)^{\mathbf{u} \cdot \mathbf{x} + \mathbf{c} \cdot \mathbf{y}} i^{wt(\mathbf{c} \odot \mathbf{x})} .$$

Proof. We first show that $\chi_{\mathbf{u}, \mathbf{c}} : G \rightarrow \mathbb{C}$ is a group homomorphism. For $\mathbf{u}, \mathbf{c} \in \mathbb{F}_2^n$ we have

$$\begin{aligned} \chi_{\mathbf{u}, \mathbf{c}}((\mathbf{x}_1, \mathbf{y}_1) * (\mathbf{x}_2, \mathbf{y}_2)) &= \chi_{\mathbf{u}, \mathbf{c}}(\mathbf{x}_1 + \mathbf{x}_2, \mathbf{y}_1 + \mathbf{y}_2 + \mathbf{x}_1 \odot \mathbf{x}_2) \\ &= (-1)^{\mathbf{u} \cdot (\mathbf{x}_1 + \mathbf{x}_2) + \mathbf{c} \cdot (\mathbf{y}_1 + \mathbf{y}_2 + \mathbf{x}_1 \odot \mathbf{x}_2)} i^{wt(\mathbf{c} \odot (\mathbf{x}_1 + \mathbf{x}_2))} . \end{aligned}$$

On the other hand,

$$\chi_{\mathbf{u}, \mathbf{c}}(\mathbf{x}_1, \mathbf{y}_1) \chi_{\mathbf{u}, \mathbf{c}}(\mathbf{x}_2, \mathbf{y}_2) = (-1)^{\mathbf{u} \cdot (\mathbf{x}_1 + \mathbf{x}_2) + \mathbf{c} \cdot (\mathbf{y}_1 + \mathbf{y}_2)} i^{wt(\mathbf{c} \odot \mathbf{x}_1) + wt(\mathbf{c} \odot \mathbf{x}_2)} .$$

Hence we conclude that $\chi_{\mathbf{u}, \mathbf{c}}((\mathbf{x}_1, \mathbf{y}_1) * (\mathbf{x}_2, \mathbf{y}_2)) = \chi_{\mathbf{u}, \mathbf{c}}(\mathbf{x}_1, \mathbf{y}_1) \chi_{\mathbf{u}, \mathbf{c}}(\mathbf{x}_2, \mathbf{y}_2)$ if and only if

$$i^{2\mathbf{c} \cdot (\mathbf{x}_1 \odot \mathbf{x}_2) + wt(\mathbf{c} \odot (\mathbf{x}_1 + \mathbf{x}_2))} = i^{wt(\mathbf{c} \odot \mathbf{x}_1) + wt(\mathbf{c} \odot \mathbf{x}_2)} ,$$

or equivalently

$$2\mathbf{c} \cdot (\mathbf{x}_1 \odot \mathbf{x}_2) + wt(\mathbf{c} \odot (\mathbf{x}_1 + \mathbf{x}_2)) \equiv wt(\mathbf{c} \odot \mathbf{x}_1) + wt(\mathbf{c} \odot \mathbf{x}_2) \pmod{4} . \quad (7)$$

With

$$\begin{aligned} wt(\mathbf{c} \odot (\mathbf{x}_1 + \mathbf{x}_2)) &= wt(\mathbf{c} \odot \mathbf{x}_1 + \mathbf{c} \odot \mathbf{x}_2) \\ &= wt(\mathbf{c} \odot \mathbf{x}_1) + wt(\mathbf{c} \odot \mathbf{x}_2) - 2wt(\mathbf{c} \odot \mathbf{x}_1 \odot \mathbf{x}_2) , \end{aligned}$$

we see that Equation (7) holds if and only if

$$2\mathbf{c} \cdot (\mathbf{x}_1 \odot \mathbf{x}_2) \equiv 2wt(\mathbf{c} \odot \mathbf{x}_1 \odot \mathbf{x}_2) \pmod{4} ;$$

that is $\mathbf{c} \cdot (\mathbf{x}_1 \odot \mathbf{x}_2) \equiv wt(\mathbf{c} \odot \mathbf{x}_1 \odot \mathbf{x}_2) \pmod{2}$, which trivially holds.

It remains to show that $\chi(\mathbf{u}_1, \mathbf{c}_1) \neq \chi(\mathbf{u}_2, \mathbf{c}_2)$ if $(\mathbf{u}_1, \mathbf{c}_1) \neq (\mathbf{u}_2, \mathbf{c}_2)$. Suppose that $\chi(\mathbf{u}_1, \mathbf{c}_1) = \chi(\mathbf{u}_2, \mathbf{c}_2)$, which yields

$$(-1)^{(\mathbf{u}_1 + \mathbf{u}_2) \cdot \mathbf{x} + (\mathbf{c}_1 + \mathbf{c}_2) \cdot \mathbf{y}} i^{wt(\mathbf{c}_1 \odot \mathbf{x}) - wt(\mathbf{c}_2 \odot \mathbf{x})} = 1 \quad (8)$$

for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_2^n$. If (8) holds, then $wt(\mathbf{c}_1 \odot \mathbf{x}) - wt(\mathbf{c}_2 \odot \mathbf{x}) \equiv 0 \pmod{2}$. Let $\mathbf{c}_1 = (c_{1,1}, \dots, c_{1,n})$, $\mathbf{c}_2 = (c_{2,1}, \dots, c_{2,n})$, suppose that w.l.o.g., $c_{1,1} \neq c_{2,1}$, and let $\mathbf{x} = (1, 0, \dots, 0)$. Then $wt(\mathbf{c}_1 \odot \mathbf{x}) - wt(\mathbf{c}_2 \odot \mathbf{x}) = \pm 1$. We conclude that Equation (8) implies $\mathbf{c}_1 = \mathbf{c}_2$. Equation (8) then implies $(-1)^{(\mathbf{u}_1 + \mathbf{u}_2) \cdot \mathbf{x}} = 1$ for all $\mathbf{x} \in \mathbb{F}_2^n$, thus $\mathbf{u}_1 = \mathbf{u}_2$. \square

Let f be a function on \mathbb{F}_2^n . By the characterization of RDSs via characters in Equation (1), the set $\{(\mathbf{x}, f(\mathbf{x})) : \mathbf{x} \in \mathbb{F}_2^n\}$ is a $(2^n, 2^n, 2^n, 1)$ -RDS in G if and only if for every $\mathbf{c}, \mathbf{u} \in \mathbb{F}_2^n$, $\mathbf{c} \neq \mathbf{0}$,

$$\left| \sum_{\mathbf{x} \in \mathbb{F}_2^n} \chi_{\mathbf{u}, \mathbf{c}}(\mathbf{x}, f(\mathbf{x})) \right| = \left| \sum_{\mathbf{x} \in \mathbb{F}_2^n} (-1)^{\mathbf{c} \cdot f(\mathbf{x}) + \mathbf{u} \cdot \mathbf{x}} i^{wt(\mathbf{c} \odot \mathbf{x})} \right| = |\mathcal{U}_{f_{\mathbf{c}}}^{\mathbf{c}}(\mathbf{u})| = 2^{n/2},$$

where $f_{\mathbf{c}}$ denotes the component function $f_{\mathbf{c}}(\mathbf{x}) = \mathbf{c} \cdot f(\mathbf{x})$ of f . Note that $|\sum_{\mathbf{x} \in \mathbb{F}_2^n} \chi_{\mathbf{0}, \mathbf{0}}(\mathbf{x}, f(\mathbf{x}))| = 2^n$ and $|\sum_{\mathbf{x} \in \mathbb{F}_2^n} \chi_{\mathbf{u}, \mathbf{0}}(\mathbf{x}, f(\mathbf{x}))| = 0$ if $\mathbf{u} \neq \mathbf{0}$, trivially hold. We obtain the following theorem.

Theorem 4. *The function $f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ is a modified planar function if and only if for every nonzero $\mathbf{c} \in \mathbb{F}_2^n$ the component function $f_{\mathbf{c}}$ is a \mathbf{c} -bent₄ function.*

Proof. By the above discussion, both conditions are equivalent to $\{(\mathbf{x}, f(\mathbf{x})) : \mathbf{x} \in \mathbb{F}_2^n\}$ being a $(2^n, 2^n, 2^n, 1)$ -RDS in G . \square

The equivalence of the conditions

- (i) $f(\mathbf{x}) + f(\mathbf{x} + \mathbf{a}) + \mathbf{a} \odot \mathbf{x}$ is a permutation for every nonzero \mathbf{a} , and
- (ii) for every nonzero \mathbf{c} the component function $f_{\mathbf{c}}$ is \mathbf{c} -bent₄,

can of course also be deduced directly. As for the analog conditions for planar functions in odd characteristic, by squaring the respective transform one first shows that a function $g : \mathbb{F}_2^n \rightarrow \mathbb{F}_2$ is \mathbf{c} -bent₄ if and only if

$$g(\mathbf{x}) + g(\mathbf{x} + \mathbf{z}) + \mathbf{c} \cdot (\mathbf{z} \odot \mathbf{x}) \quad (9)$$

is balanced for all nonzero $\mathbf{z} \in \mathbb{F}_2^n$. We omit this argument at this position and include it in the next section, where we deal with modified planar functions in univariate form.

3 Components of univariate modified planar functions

So far, all known examples of modified planar functions are in univariate representation; i.e. they are univariate functions f satisfying Equation (4), hence induce RDSs in the group $G = (\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \star)$ with the operation $(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + x_1 x_2)$. Trivial examples are all affine functions. Besides from affine functions, all known examples of modified planar functions are quadratic functions (represented by Dembowski-Ostrom polynomials). The existence of a nonquadratic modified planar function is an open problem.

To analyse component functions of modified planar functions on \mathbb{F}_{2^n} , we first determine the group of characters of G . For $c, x \in \mathbb{F}_{2^n}$ we define

$$\sigma(c, x) := \sum_{0 \leq i < j \leq n-1} (cx)^{2^i} (cx)^{2^j}.$$

Note that $\sigma(c, x)^2 = \sigma(c, x)$, and hence $\sigma(c, x)$ is a Boolean function.

Lemma 5. *For $c, x_1, x_2 \in \mathbb{F}_{2^n}$ we have*

$$\sigma(c, x_1 + x_2) = \sigma(c, x_1) + \sigma(c, x_2) + \text{Tr}_n(cx_1)\text{Tr}_n(cx_2) + \text{Tr}_n(c^2 x_1 x_2).$$

Proof. Expanding $\sigma(c, x_1 + x_2)$, we get the desired conclusion as follows.

$$\begin{aligned} & \sigma(c, x_1 + x_2) \\ &= \sum_{i < j} (c(x_1 + x_2))^{2^i} (c(x_1 + x_2))^{2^j} \\ &= \sum_{i < j} (cx_1)^{2^i} (cx_1)^{2^j} + \sum_{i < j} (cx_2)^{2^i} (cx_2)^{2^j} + \sum_{i < j} ((cx_1)^{2^i} (cx_2)^{2^j} + (cx_1)^{2^j} (cx_2)^{2^i}) \\ &= \sigma(c, x_1) + \sigma(c, x_2) + \sum_{i, j} (cx_1)^{2^i} (cx_2)^{2^j} + \sum_i (cx_1)^{2^i} (cx_2)^{2^i} \\ &= \sigma(c, x_1) + \sigma(c, x_2) + \left(\sum_i (cx_1)^{2^i} \right) \left(\sum_j (cx_2)^{2^j} \right) + \sum_i (c^2 x_1 x_2)^{2^i} \\ &= \sigma(c, x_1) + \sigma(c, x_2) + \text{Tr}_n(cx_1)\text{Tr}_n(cx_2) + \text{Tr}_n(c^2 x_1 x_2). \end{aligned}$$

□

Proposition 6. *Let $G = (\mathbb{F}_{2^n} \times \mathbb{F}_{2^n}, \star)$ be the group with the operation $(x_1, y_1) \star (x_2, y_2) = (x_1 + x_2, y_1 + y_2 + x_1 x_2)$. Then the group of characters*

of G is $\chi_G = \{\chi_{u,c} : u, c \in \mathbb{F}_{2^n}\}$, where

$$\chi_{u,c}(x, y) = (-1)^{\text{Tr}_n(ux) + \text{Tr}_n(c^2y) + \sigma(c,x)} i^{\text{Tr}_n(cx)}.$$

Proof. With the definition of $\chi_{u,c}$, we see that the equality

$$\chi_{u,c}((x_1, y_1) \star (x_2, y_2)) = \chi_{u,c}(x_1, y_1) \chi_{u,c}(x_2, y_2)$$

holds if and only if

$$(-1)^{\sigma(c,x_1) + \sigma(c,x_2)} i^{\text{Tr}_n(cx_1) + \text{Tr}_n(cx_2)} = (-1)^{\text{Tr}_n(c^2x_1x_2) + \sigma(c,x_1+x_2)} i^{\text{Tr}_n(c(x_1+x_2))},$$

or equivalently

$$2\sigma(c, x_1) + 2\sigma(c, x_2) + \text{Tr}_n(cx_1) + \text{Tr}_n(cx_2) \equiv 2\text{Tr}_n(c^2x_1x_2) + 2\sigma(c, x_1 + x_2) + \text{Tr}_n(c(x_1 + x_2)) \pmod{4}. \quad (10)$$

With the identity

$$\text{Tr}_n(x) + \text{Tr}_n(y) \equiv \text{Tr}_n(x + y) + 2\text{Tr}_n(x)\text{Tr}_n(y) \pmod{4}, \quad (11)$$

Condition (10) is equivalent to

$$2\sigma(c, x_1) + 2\sigma(c, x_2) + 2\text{Tr}_n(cx_1)\text{Tr}_n(cx_2) \equiv 2\text{Tr}_n(c^2x_1x_2) + 2\sigma(c, x_1 + x_2) \pmod{4};$$

i.e. $\sigma(c, x_1) + \sigma(c, x_2) + \text{Tr}_n(cx_1)\text{Tr}_n(cx_2) + \text{Tr}_n(c^2x_1x_2) \equiv \sigma(c, x_1 + x_2) \pmod{2}$, which is true by Lemma 5.

It remains to show that $\chi_{u_1,c_1} \neq \chi_{u_2,c_2}$ if $(u_1, c_1) \neq (u_2, c_2)$. Suppose that $\chi_{u_1,c_1} = \chi_{u_2,c_2}$; i.e.

$$(-1)^{\text{Tr}_n((u_1-u_2)x) + \text{Tr}_n((c_1^2-c_2^2)y) + \sigma(c_1x) + \sigma(c_2x)} i^{\text{Tr}_n(c_1x) - \text{Tr}_n(c_2x)} = 1 \quad (12)$$

for all $x \in \mathbb{F}_{2^n}$. Observe that (modulo 4), $\text{Tr}_n(c_1x) - \text{Tr}_n(c_2x) \in \{-1, 0, 1\}$. As a result, Equation (12) implies that $\text{Tr}_n(c_1x) - \text{Tr}_n(c_2x) = 0$ for all $x \in \mathbb{F}_{2^n}$, which implies $c_1 = c_2$. Immediately one sees that then $u_1 = u_2$. \square

Knowing the group of characters, we can employ the character sum characterization of RDSs in Equation (1) to obtain conditions for functions $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ for which the graph of f is an RDS in G . Observing that $|\sum_{x \in \mathbb{F}_{2^n}} \chi_{0,0}(x, f(x))| = 2^n$ and $|\sum_{x \in \mathbb{F}_{2^n}} \chi_{u,0}(x, f(x))| = 0$ if $u \neq 0$, are

again trivially satisfied, the set $\{(x, f(x)) : x \in \mathbb{F}_{2^n}\}$ is an RDS in G if and only if for every $u, c \in \mathbb{F}_{2^n}$, $c \neq 0$, we have

$$\left| \sum_{x \in \mathbb{F}_{2^n}} \chi_{u,c}(x, f(x)) \right| = \left| \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}_n(c^2 f(x)) + \sigma(c,x)} i^{\text{Tr}_n(cx)} (-1)^{\text{Tr}_n(ux)} \right| = 2^{n/2}.$$

This motivates the definition of a unitary transform \mathcal{V}_g^c , $c \in \mathbb{F}_{2^n}$, for a function $g : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ as

$$\mathcal{V}_g^c(u) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{g(x) + \sigma(c,x)} i^{\text{Tr}_n(cx)} (-1)^{\text{Tr}_n(ux)}.$$

Note that for $c = 0$, we again obtain the conventional Walsh-Hadamard transform for univariate Boolean functions. We define the nega-Hadamard transform for univariate functions as \mathcal{V}_g^c for $c = 1$.

As the graph of f is a $(2^n, 2^n, 2^n, 1)$ -RDS in G if and only if for all nonzero $c \in \mathbb{F}_{2^n}$ the component function $f_{c^2}(x) = \text{Tr}_n(c^2 f(x))$ of f has a flat spectrum with respect to \mathcal{V}_g^c , we find it natural to define bent₄ functions in univariate form by using these transforms.

Definition 7. *A function $g : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ is called bent₄ if it has a flat spectrum with respect to at least one of the transforms \mathcal{V}_g^c . In other words, g is bent₄ if there exists an element $c \in \mathbb{F}_{2^n}$ such that $|\mathcal{V}_g^c(u)| = 2^{n/2}$ for all $u \in \mathbb{F}_{2^n}$.*

The functions from \mathbb{F}_{2^n} to \mathbb{F}_2 with a flat spectrum with respect to \mathcal{V}_g^0 are the bent functions. In accordance with the case of multivariate functions we call a function with a flat spectrum with respect to \mathcal{V}_g^1 a negabent function. With this notations we obtain a univariate analog of Theorem 4.

Theorem 8. *A function $f : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is a modified planar function if and only if for every nonzero $c \in \mathbb{F}_{2^n}$ the component function $f_{c^2}(x) = \text{Tr}_n(c^2 f(x))$ is a c -bent₄ function.*

Note that $c \rightarrow c^2$ is a permutation of the multiplicative group of \mathbb{F}_{2^n} , and hence Theorem 8 gives a condition on all component functions of f .

We finally show the equivalence of the condition in Theorem 8 and Condition (4) directly, which may also provide us a further understanding of component functions of modified planar functions. As for the case of conventional bent functions we follow the approach via Hadamard matrices, see e.g. [3].

Lemma 9. *Let h be a complex valued function on \mathbb{F}_{2^n} . Then*

$$\Psi(u) = \sum_{z \in \mathbb{F}_{2^n}} h(z) (-1)^{\text{Tr}_n(uz) + \sigma(c,z)} i^{\text{Tr}_n(cz)} = h(0)$$

for all $u \in \mathbb{F}_{2^n}$, if and only if $h(z) = 0$ for $z \neq 0$.

Theorem 10. *A function $g : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ is a c -bent₄ function if and only if*

$$g(x) + g(x+z) + \text{Tr}_n(c^2xz)$$

is balanced for all $z \neq 0$.

Proof. For every $u \in \mathbb{F}_{2^n}$ we have

$$\mathcal{V}_g^c(u) \overline{\mathcal{V}_g^c(u)} = \sum_{z \in \mathbb{F}_{2^n}} (-1)^{\text{Tr}_n(uz) + \sigma(c,z)} i^{\text{Tr}_n(cz)} \sum_{x \in \mathbb{F}_{2^n}} (-1)^{g(x) + g(x+z) + \text{Tr}_n(c^2xz)}, \quad (13)$$

where $\overline{\mathcal{V}_g^c(u)}$ is the complex conjugate of $\mathcal{V}_g^c(u)$. Hence we conclude that if $g(x) + g(x+z) + \text{Tr}_n(c^2xz)$ is balanced, then $\mathcal{V}_g^c(u) \overline{\mathcal{V}_g^c(u)} = 2^n$; i.e. g is c -bent₄.

Conversely suppose that g is c -bent₄, thus $\mathcal{V}_g^c(u) \overline{\mathcal{V}_g^c(u)} = 2^n$. Setting

$$h(z) := \sum_{x \in \mathbb{F}_{2^n}} (-1)^{g(x) + g(x+z) + \text{Tr}_n(c^2xz)},$$

with Equation (13) this yields

$$\sum_{z \in \mathbb{F}_{2^n}} h(z) (-1)^{\text{Tr}_n(uz) + \sigma(c,z)} i^{\text{Tr}_n(cz)} = h(0) = 2^n.$$

By Lemma 9, this implies that $h(z) = 0$ for every nonzero z , which holds if and only if $g(x) + g(x+z) + \text{Tr}_n(c^2xz)$ is balanced for every $z \neq 0$. \square

The function $h : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_{2^n}$ is a permutation if and only if for every nonzero $c \in \mathbb{F}_2^n$, $\text{Tr}_n(ch)$ is balanced (see [8, Theorem 7.7]). This yields the desired result given in the following corollary.

Corollary 11. *Let f be a function on \mathbb{F}_{2^n} . Then $\text{Tr}_n(c^2f)$ is c -bent₄ for all nonzero $c \in \mathbb{F}_{2^n}$ if and only if $f(x) + f(x+z) + xz$ is a permutation for all nonzero $z \in \mathbb{F}_{2^n}$*

Remark 12. *Univariate bent₄ functions defined as in Definition 7 behave somewhat different than the multivariate bent₄ functions in Definition 2. Observe that every affine function $f(x) = \text{Tr}_n(ax) + b$, $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_2$, is c -bent₄ for every nonzero c . Affine functions in multivariate form are trivial examples for negabent functions (see also [9, Proposition 1]). But a multivariate affine function is never \mathbf{c} -bent₄ for any $\mathbf{c} \neq \mathbf{1}$: As easily seen, Equation (9) is constant for an affine function g if one chooses $\mathbf{z} = (z_1, \dots, z_n)$ such that $z_i = 0$ if $c_i = 1$.*

Remark 13. *In [13, 21] a negabent function $g : \mathbb{F}_{2^n} \rightarrow \mathbb{F}_2$ is defined to be a function for which $g(x) + g(x+z) + \text{Tr}_n(xz)$ is balanced for all nonzero z . This is equivalent with our definition of a negabent function as a function with a flat spectrum with respect to \mathcal{V}_g^1 .*

4 Acknowledgment

Nurdagül Anbar gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF-4002-00367) and H.C. Ørsted COFUND Post-doc Fellowship from the project “Algebraic curves with many rational points”.

Wilfried Meidl is supported by the Austrian Science Fund (FWF) Project no. M 1767-N26.

References

- [1] A. Blokhuis, D. Jungnickel, B. Schmidt, Proof of the prime power conjecture for projective planes of order n with abelian collineation groups of order n^2 . Proc. Amer. Math. Soc. 130 (2002), no. 5, 1473–1476.
- [2] P. Dembowski, T.G. Ostrom, Planes of order n with collineation groups of order n^2 . Math. Z. 103 (1968) 239–258.
- [3] J.F. Dillon, Elementary Hadamard difference sets, Ph.D. dissertation, University of Maryland, 1974.
- [4] S. Gangopadhyay, E. Pasalic, P. Stănică, A note on generalized bent criteria for Boolean functions. IEEE Trans. Inform. Theory 59 (2013), no. 5, 3233–3236.
- [5] M.J. Ganley, E. Spence, Relative difference sets and quasiregular collineation groups. J. Combinatorial Theory Ser. A 19 (1975), no. 2, 134–153.

- [6] M.J. Ganley, On a paper of P. Dembowski and T. G. Ostrom: "Planes of order n with collineation groups of order n^2 ". Arch. Math. (Basel) 27 (1976), no. 1, 93–98.
- [7] P.V. Kumar, R.A. Scholtz, L.R. Welch, Generalized bent functions and their properties. J. Combin. Theory Ser. A 40 (1985), no. 1, 90–107.
- [8] R. Lidl, H. Niederreiter, Finite Fields, 2nd ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, Cambridge, (1997).
- [9] M.G. Parker, A. Pott, On Boolean functions which are bent and negabent. Sequences, subsequences, and consequences, 9–23, Lecture Notes in Comput. Sci., 4893, Springer, Berlin, 2007.
- [10] A. Pott, K.U. Schmidt, Y. Zhou, Semifields, relative difference sets, and bent functions. Algebraic curves and finite fields, 161–178, Radon Ser. Comput. Appl. Math., 16, De Gruyter, Berlin, 2014.
- [11] A. Pott, Almost perfect and planar functions, Des. Codes Cryptogr. 78 (2016), 141–195.
- [12] C. Riera, M.G. Parker, Generalized bent criteria for Boolean functions. I. IEEE Trans. Inform. Theory 52 (2006), no. 9, 4142–4159.
- [13] S. Sarkar, Characterizing negabent Boolean functions over finite fields. Sequences and their applications SETA 2012, 7788, Lecture Notes in Comput. Sci., 7280, Springer, Heidelberg, 2012.
- [14] K.U. Schmidt, M.G. Parker, A. Pott, Negabent functions in the Maiorana-McFarland class. Sequences and their applications SETA 2008, 390402, Lecture Notes in Comput. Sci., 5203, Springer, Berlin, 2008.
- [15] K.U. Schmidt, Y. Zhou, Planar functions over fields of characteristic two. J. Algebraic Combin. 40 (2014), no. 2, 503–526.
- [16] P. Stănică, S. Gangopadhyay, A. Chaturvedi, A.K. Gangopadhyay, S. Maitra, Investigations on bent and negabent functions via the nega-Hadamard transform, IEEE Trans. Inform. Theory 58 (2012), 4064–4072.
- [17] W. Su, A. Pott, X. Tang, Characterization of negabent functions and construction of bent-negabent functions with maximum algebraic degree. IEEE Trans. Inform. Theory 59 (2013), 3387–3395.

- [18] Y. Tan, A. Pott, T. Feng, Strongly regular graphs associated with ternary bent functions. *J. Combin. Theory Ser. A* 117 (2010), no. 6, 668–682.
- [19] F. Zhang, Y. Wei, E. Pasalic, Constructions of bent-negabent functions and their relation to the completed Maiorana-McFarland class. *IEEE Trans. Inform. Theory* 61 (2015), 1496–1506.
- [20] Y. Zhou, $(2n, 2n, 2n, 1)$ -relative difference sets and their representations. *J. Combin. Des.* 21 (2013), no. 12, 563–584.
- [21] Y. Zhou, L. Qu, Constructions of negabent functions over finite fields, *Cryptography and Communications*, to appear.